

# PRIVACY IMPACT ASSESSMENT

(Rev. 2/2020)

(All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official. *All entries must be Times New Roman, 12pt, and start on the next line.* If you need further assistance, contact your LPO. A listing of the LPOs can be found here:

[https://usepa.sharepoint.com/:w:/r/sites/oei\\_Community/OISP/Privacy/LPODoc/LPO%20Roster.docx](https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO%20Roster.docx)

<b>System Name:</b> RCRA Information System with e-Manifest Module (RCRAInfo)	<b>System Owner:</b> Carolyn Hoskinson, ORCR Director
<b>Preparer:</b> Thomas Reaves	<b>Office:</b> OLEM/ORCR
<b>Date:</b> February 18, 2021	<b>Phone:</b> 703-308-7281
<b>Reason for Submittal:</b> New PIA <input checked="" type="checkbox"/> Revised PIA <input type="checkbox"/> Annual Review <input type="checkbox"/> Rescindment <input type="checkbox"/>	
<b>This system is in the following life cycle stage(s):</b>	
Definition <input type="checkbox"/> Development/Acquisition <input type="checkbox"/> Implementation <input type="checkbox"/>	
Operation & Maintenance <input checked="" type="checkbox"/> Rescindment/Decommissioned <input type="checkbox"/>	
<b>Note: New and Existing Systems require a PIA annually, when there is a significant modification to the system or where privacy risk has increased to the system. For examples of significant modifications, see <u>OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).</u></b>	
<b>The PIA must describe the risk associated with that action. For assistance in applying privacy risk see <u><a href="#">OMB Circular No. A-123, Section VII (A) (pgs. 44-45).</a></u></b>	

## **Provide a general description/overview and purpose of the system:**

The Resource Conservation and Recovery Act (RCRA) necessitated creation of an information system to address hazardous waste tracking. The RCRA Information System combines various hazardous waste tracking and monitoring functionalities into an overarching information system. Major functionalities within the system include RCRAInfo, the e-Manifest module, and the Waste Imports and Exports Tracking System (WIETS) module. The Information System is hosted within the Amazon Web Services (AWS) US East Hosting environment and is directly connected to the EPA enterprise via dedicated Office of Mission Support (OMS) designed, implemented, monitored and maintained Trusted Internet Connection (TIC) compliant, Virtual Private Network (VPN) connections. The OMS provided TIC compliant VPN connections establish direct links from the AWS hosting environment to the EPA enterprise and provides the single point of entry/exit for all RCRA Information System components.

The RCRA Information System Hosting Environment also includes public facing components (RCRAInfo

Web and RCRA Online). Unlike the modules mentioned above, which require all users to authenticate (log in with username/password), public facing components do not require authentication. Notwithstanding authentication requirements, all traffic to/from the RCRA Information System Hosting environment traverses the TIC compliant VPN and is therefore subjected to additional security and compliance monitoring.

The RCRA Information System supports the Agency's mission by improving access to hazardous waste information; continuing to reduce the burden to data providers by leveraging cutting edge technology to support identified data access needs; and providing a platform which supports the integration of national and transboundary hazardous waste data and data flows into the Agency's enterprise architecture. e-Manifest extends this functionality addressing the facilitation of electronic transmission of the Uniform Hazardous Waste Manifest form (EPA Form 8700-22) making a less burdensome, more cost-effective, and convenient process for industry users. WIETS facilitates incorporation of the international import/export tracking of hazardous waste shipments into an integrated system and leverages the existing, robust architectural platform.

## **Section 1.0 Authorities and Other Requirements**

### **1.1 What specific legal authorities and/or Executive Order(s) permit and define the collection of information by the system in question?**

RCRAInfo is EPA's comprehensive information system, providing access to data supporting the Resource Conservation and Recovery Act (RCRA) of 1976 and the Hazardous and Solid Waste Amendments (HSWA) of 1984<sup>1</sup>.

Per the e-Manifest Final Rule<sup>2</sup>, the information is being collected to facilitate implementation of certain provisions of the Hazardous Waste Electronic Manifest Establishment Act, Public Law 112–195<sup>3</sup> (the e-Manifest Act), which directs EPA to establish a national electronic manifest system.

WIETS is defined by 42 U.S. Code § 6938<sup>4</sup> provides the basis for the regulations found in Title 40 Protection of the Environment, Chapter I, Subchapter I, Part 262, Subpart H - Transboundary Movements of Hazardous Waste for Recovery or Disposal,<sup>5</sup> and through ratification by the US Senate of the Basel Convention on the Control of Transboundary Movements of Hazardous Wastes and Their Disposal, with Annexes, done at Basel on March 22, 1989<sup>6</sup>.

### **1.2 Has a system security plan been completed for the information system(s) supporting the system? Does the system have or will the system be issued**

### **an Authorization-to-Operate? When does the ATO expire?**

A System Security Plan has been completed. An ATO has been issued. The current RCRA Information System ATO expires 5/11/2021.

### **1.3 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.**

e-Manifest is covered by OMB No. 2050-0039, EPA Form 8700-22 (3), EPA Form 8700-22A (4).

### **1.4 Will the data be maintained or stored in a Cloud? If so, is the Cloud Service Provider (CSP) FedRamp approved? What type of service (PaaS, IaaS, SaaS, etc.) will the CSP provide?**

Yes, Data is cloud based. The CSP is FedRAMP certified and providing IaaS for the system.

## **Section 2.0 Characterization of the Information**

*The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.*

### **2.1 Identify the information the system collects, uses, disseminates, or maintains (e.g., data elements, including name, address, DOB, SSN).**

The system collects data associated with processing electronic Uniform Hazardous Waste Manifests (EPA Form 8700-22), and (if necessary) the associated Continuation Sheet (EPA Form 8700-22A), and data associated with processing transboundary shipments of hazardous wastes. Privacy data stored in the system consists of the name of the waste Generator, name of the waste Transporter(s), and name of the waste Treatment, Storage, and Disposal Facility (TSDf or Designated Facility) receiving party. All other manifest data that is stored is directly related to waste handler entities and waste stream processing activities.

### **2.2 What are the sources of the information and how is the information collected for the system?**

The data sources for manifests and transboundary movement documents are the individuals and/or information systems who work for companies involved in the generation, transport and treatment, storage, and/or disposal of waste streams.

There are two methods for electronically collecting manifest data:

- a) Users can log into the e-Manifest system to process hazardous waste manifests. Generators, Brokers (acting on-behalf of Generators), Transporters, and TSDf personnel can enter manifest data directly into the system via a web browser.
- b) TSDfs can process manifest data and necessary transboundary movement documents via secure Application Programming Interfaces (APIs) (system to system connections)

with the RCRA Information System back-end. As with the first method, TSDf access is limited to only those manifests and associated documents/data to which they are a party.

### **2.3 Does the system use information from commercial sources or publicly available data? If so, explain why and how this information is used.**

Yes. The system exists to allow commercial entities to process hazardous waste manifests and transboundary movement documents. States monitoring hazardous waste shipments can/do publish manifest data on various state sites today. Per the e-Manifest Final Rule, “after the 90-day period of restricted access has passed, the Agency intends to provide full direct, on-line access by the public to all manifest data in the system”. (5)

The WIETS module information is used to meet the statutory requirements associated with the hazardous waste import/export process (Title 40 Protection of the Environment, Chapter I, Subchapter I, Part 262, Subpart H - Transboundary Movements of Hazardous Waste for Recovery or Disposal).

### **2.4 Discuss how accuracy of the data is ensured.**

For manifest data, prior to making manifests publicly available, the 90-day period for corrections and verifications serves as an opportunity for users to ensure accuracy. Manifests serve as historical records for hazardous waste handling. As such, the information contained in the manifest is deemed sufficiently accurate, relevant, timely and complete until legal disposal. Electronic manifest processing involves logging of any/every action performed against a manifest which ensures any alterations are properly and sufficiently accounted for.

For WIETS, system users are responsible for providing the information in WIETS module. The information contained in the system is deemed sufficiently accurate, relevant, timely and complete upon user entry/edit. WIETS processing involves logging of any/every action performed which ensures any alterations are properly and sufficiently accounted for.

### **2.5 Privacy Impact Analysis: Related to Characterization of the Information**

*Discuss the privacy risks identified for the specific data elements and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.*

#### **Privacy Risk:**

The system collects and stores the name of the waste handler responsible party. While this information may be publicly available through generic search engines (i.e. Google, Bing, etc.), it could potentially be used to tie an individual to a specific employer and/or state.

#### **Mitigation:**

All applicable NIST 800-53 rev.4 Security and Privacy controls are implemented to ensure protection commensurate with the system categorization. EPA has minimized the risk of unauthorized access to the system by establishing a secure environment for exchanging electronic

information. The system is housed within a FedRAMP Moderate level certified, CSP controlled entry area, within a secured facility. Additionally, multiple levels of security are maintained with the computer system control program. This system limits data access to authorized individuals on a need to know/access basis, and controls individuals' ability to access and alter records with the system. All users of the system are given a unique user identification (ID) with personal identifiers, and all interactions between the system and the authorized individual users are logged.

## **Section 3.0 Access and Data Retention by the System**

*The following questions are intended to outline the access controls for the system and how long the system retains the information after the initial collection.*

### **3.1 Do the systems have access control levels within the system to prevent authorized users from accessing information they don't have a need to know? If so, what control levels have been put in place? If no controls are in place why have they been omitted?**

Yes. The system applies the applicable controls of the Low baseline of NIST 800-53 rev.4 Access Control (AC) family and all associated and applicable Agency prescribed Privacy controls. Controls to prevent access to role-restricted information is via system implemented Role Based Access Controls. Individual users request a role within the system. Permissions associated with the role are applied when the Role Request is approved/denied by a system manager. The applicable permission levels are Create, Read, Update, Delete (CRUD) and are applied based on user roles.

### **3.2 In what policy/procedure are the access controls identified in 3.1, documented?**

NIST 800-53 rev.4 as prescribed in the EPA Information Security and Privacy Control Guide Rev 4-FY21.

### **3.3 Are there other components with assigned roles and responsibilities within the system?**

No.

### **3.4 Who (internal and external parties) will have access to the data/information in the system? If contractors, are the appropriate Federal Acquisition Regulation (FAR) clauses included in the contract?**

Internally, members of the RCRA Information System team/administrators (government and contract employees) will have access to the data/information in the system. During manifest processing, EPA regional employees, external users from the impacted states, and external registered handling parties will have access to the data/information related to manifests and transboundary import/export documents to which they are a party.

After the initial 90-day period for corrections, per the Final Rule, "the Agency intends to provide full direct, on-line access by the public to all [releasable] manifest data in the system".

FAR Clauses 52.224-1 and 52.224-2 are both included by reference in the base contracts (and are therefore applicable to any resultant task orders).

### **3.5 Explain how long and for what reasons the information is retained. Does the system have an EPA Records Control Schedule? If so, provide the schedule number.**

Manifests and transboundary shipping documents serve as historical records for hazardous waste handling. The applicable record schedule is 0257. Records in the system under this schedule are Permanent (NARA Disposal Authority: N1-412-04-8c, NARA Disposal Authority: N1-412-04-8d).

### **3.6 Privacy Impact Analysis: Related to Retention**

*Discuss the risks associated with the length of time data is retained. How were those risks mitigated? The schedule should align the stated purpose and mission of the system.*

#### **Privacy Risk:**

The privacy risk is the potential of keeping records longer than their actual retention timeframe. While this information may be publicly available through generic search engines (i.e. Google, Bing, etc.), during the pre-release period (90 days), it could be used to tie an individual to a specific employer and/or state. By Congressional mandate, the data in the system is released to the public after the 90-day corrections and verification period. Privacy risks related to retention are relieved once the data is released to the public domain.

#### **Mitigation:**

System data is transferred to NARA on an annual basis. However, data is publicly releasable after 90 days. Also, all applicable NIST 800-53 rev.4 Security and Privacy controls are implemented to ensure protection commensurate with the system categorization. The system has minimized the risk associated with access and data retention by establishing a secure environment for storing current system information within the FedRAMP Moderate AWS US East facilities.

## **Section 4.0 Information Sharing**

*The following questions are intended to describe the scope of the system information sharing external to the Agency. External sharing encompasses sharing with other federal, state and local government, and third-party private sector entities.*

### **4.1 Is information shared outside of EPA as part of the normal agency operations? If so, identify the organization(s), how the information is accessed and how it is to be used, and any agreements that apply.**

Yes. Initially the impacted states and registered handling parties will have access to the data/information related to manifests and/or transboundary documents to which they are a party. In all cases, information is accessed via logging into the RCRA Information System using credentials to manage/monitor information.

As indicated in the Final Rule, after a 90-day period to allow for correction and verification of waste shipment information, “the Agency intends to provide full direct, on-line access by

the public to all [releasable] manifest data in the system”. After the initial 90-day period for corrections, per the Final Rule, “the Agency intends to provide full direct, on-line access by the public to all [releasable] manifest data in the system”. There is no need for an agreement to access public data.

#### **4.2 Describe how the external sharing is compatible with the original purposes of the collection.**

External sharing is mandated by the Hazardous Waste Electronic Manifest Establishment Act, Public Law 112–195 (the e-Manifest Act), and accordingly to transboundary waste handling which utilizes manifests to track hazardous waste.

#### **4.3 How does the system review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within EPA and outside?**

Existing agreements are reviewed as a part of the annual system security review. Inquiries for new uses/access by internal (EPA) organizations will follow the Agency established procedures for system interconnections and/or information sharing. Organizations outside of EPA (waste handlers can request an account to access their data within the system. External organizations (other than waste handlers) can only access the information after the 90-day corrections period.

#### **4.4 Does the agreement place limitations on re-dissemination?**

No. As indicated in the Final Rule, after a 90-day period to allow for correction and verification of waste shipment information, “the Agency intends to provide full direct, on-line access by the public to all [releasable] manifest data in the system”. There is no need for an agreement to access public data.

Further, for transboundary data, the external waste handling entities initiate data entry and retain visibility to their information. Only those external parties to transboundary transactions may view data associated with their own transactions. In other words, an external entity can view their own information, but not another (non-party) handler’s information.

#### **4.5 Privacy Impact Analysis: Related to Information Sharing**

*Discuss the privacy risks associated with the sharing of information outside of the agency. How were those risks mitigated?*

##### **Privacy Risk:**

The privacy risk is that some information may be exposed. The information contained within the system is to become publicly available after 90 days. The Privacy risk associated with information sharing before/after public release is minimal and commensurate with other public government data. Also, the privacy information in the system consists of first and last name. The risk of sharing this information within the realm of the transboundary participants is minimal and

limited. The risk is that during the pre-release period (90 days), it could be used to tie an individual to a specific employer and/or state. This risk is relieved once the Congressionally mandated information is release into the public domain occurs.

**Mitigation:**

All applicable NIST 800-53 rev.4 Security and Privacy controls are implemented to ensure protection commensurate with the system categorization. The system has minimized the risk associated with information sharing by establishing a secure environment for exchanging electronic information with other systems. The RCRA Information System is housed within a FedRAMP Moderate AWS secured facility. Additionally, multiple levels of security are maintained with the computer system control program. This limits data access to authorized individuals on a need to know/access basis, and controls individuals' ability to access and alter records with the system. All users (to include other systems) of the system are given a unique user identification (ID) with system identifiers, and all interactions between the e-Manifest system and all connecting systems are logged.

## **Section 5.0 Auditing and Accountability**

*The following questions are intended to describe technical and policy-based safeguards and security measures.*

### **5.1 How does the system ensure that the information is used as stated in Section 6.1?**

Throughout the system workflows, users are required to acknowledge transfer of custody of the listed wastes. This process begins with the waste generator, continues with the waste transporter(s), and ends with the acknowledgement of the TSDf. System data validation ensures that each party in the chain of custody provides the required acknowledgement and ensures compliance with hazardous waste handling regulations.

The single privacy element stored in the RCRA Information System is the user's name. Data validation limits the types of information that may be entered into the system. Roles and permissions limit the quantity and context of the information that may be retrieved from the system prior to public release.

### **5.2 Describe what privacy training is provided to users either generally or specifically relevant to the system/collection.**

All EPA employees are required to take Annual Information Security and Privacy Awareness Training which includes privacy elements. Given the public releasable nature of the data within the system, external elements must manage their privacy implementations.

### **5.3 Privacy Impact Analysis: Related to Auditing and Accountability**

**Privacy Risk:**

If system auditing and accountability measures are not implemented, data could potentially be at

risk of alteration and/or repudiation.

**Mitigation:**

Electronic manifest and transboundary shipment processing involve logging of any/every action performed against a document. All users of the system are given a unique user identification (ID) with personal identifiers, and all interactions between the system and the authorized individual users are logged. Activity logs ensure any alterations are properly and sufficiently accounted for. Audit logs are protected against unauthorized access.

## **Section 6.0 Uses of the Information**

*The following questions require a clear description of the system's use of information.*

### **6.1 Describe how and why the system uses the information.**

There are two methods for collecting manifest data:

- a) Users can log into the RCRA Information System to process hazardous waste manifests and/or transboundary movement documents. Generators, Brokers (acting on-behalf of Generators), Transporters, and TSDf personnel can enter data directly into the system.
- b) TSDFs will have the ability to process waste handling data via secure Application Programming Interfaces (APIs) (system to system connections) with the RCRA Information System back- end. As with the first method, TSDf access is limited to only those manifests to which they are a party.

The system uses the information to comply with the Hazardous Waste Electronic Manifest Establishment Act, Public Law 112–1955 (the e-Manifest Act)<sup>6</sup>, which directs EPA to establish a national electronic manifest system, and to comply with the import/export requirements cited in Title 40 Protection of the Environment, Chapter I, Subchapter I, Part 262, Subpart H - Transboundary Movements of Hazardous Waste for Recovery or Disposal.

### **6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes \_\_\_ No X. If yes, what identifier(s) will be used. (A personal identifier is a name, social security number or other identifying symbol assigned to an individual, i.e. any identifier unique to an individual. Or any identifier that can be linked or is linkable to an individual.)**

The system is designed for information retrieval by:  
Handler Identifier (Company identification number)  
Manifest Tracking # (Transaction specific identification for manifest)  
Movement Document # (Import/Export ID Number)  
Facility Name (Company Name)  
Site Name/ID (Name for specific site)  
Waste Characterization  
State/Region

### **6.3 What type of evaluation has been conducted on the probable or potential**

## **effect of the privacy of individuals whose information is maintained in the system of records?**

The system collects and stores the name of the waste handler responsible party. While this information may be publicly available through generic search engines (i.e. Google, Bing, etc.), it could be used to tie an individual to a specific employer and/or state. The waste handler name is required under the governing documentation listed in Section 1.1. Only registered users can access the non-publicly released data, an individual must be a party to a transaction to view information associated with that transaction, and all NIST applicable 800-53 rev4 and applicable EPA Privacy controls have been implemented and are assessed in accordance with OISP policies/procedures.

### **6.4 Privacy Impact Analysis: Related to the Uses of Information**

*Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.*

#### **Privacy Risk:**

The system collects and stores the name of the waste handler responsible party. While this information may be publicly available through generic search engines (i.e. Google, Bing, etc.), it could be used to tie an individual to a specific employer and/or state.

#### **Mitigation:**

All applicable NIST 800-53 rev.4 Security and Privacy controls are implemented to ensure protection commensurate with the system categorization. EPA has minimized the risk of unauthorized access to the system by establishing a secure environment for exchanging electronic information. The system is housed within a controlled entry area, within a secured facility. Additionally, multiple levels of security are maintained with the computer system control program. This system limits data access to authorized individuals on a need to know/access basis, and controls individuals' ability to access and alter records with the system. All users of the system are given a unique user identification (ID) with personal identifiers, and all interactions between the system and the authorized individual users are logged.

**\*If no SORN is required, STOP HERE.**

*The NPP will determine if a SORN is required. If so, additional sections will be required.*

## **Section 7.0 Notice**

*The following questions seek information about the system's notice to the individual about the information collected, the right to consent to uses of information, and the right to decline to provide information.*

- 7.1 How does the system provide individuals notice prior to the collection of information? If notice is not provided, explain why not.**
- 7.2 What opportunities are available for individuals to consent to uses,**

**decline to provide information, or opt out of the collection or sharing of their information?**

**7.3 Privacy Impact Analysis: Related to Notice**

*Discuss how the notice provided corresponds to the purpose of the project and the stated uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information. Describe how the project has mitigated the risks associated with potentially insufficient notice and opportunity to decline or consent.*

**Privacy Risk:**

**Mitigation:**

**Section 8.0 Redress**

*The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.*

**8.1 What are the procedures that allow individuals to access their information?**

**8.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?**

**8.3 Privacy Impact Analysis: Related to Redress**

*Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and FOIA.*

**Privacy Risk:**

**Mitigation:**